(19) **RU** (11) **2 147 790** (13) **C1**

(51) МПК[7] **H 04 K 1/00, G 06 K 19/073, G 06 F 12/14**

РОССИЙСКОЕ АГЕНТСТВО
ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ РОССИЙСКОЙ ФЕДЕРАЦИИ

(21), (22) Заявка: 97105403/09, 01.09.1995

(24) Дата начала действия патента: 01.09.1995

(30) Приоритет: 07.09.1994 US 08/303,084

(46) Дата публикации: 20.04.2000

(56) Ссылки: JP 06202864 A, 22.07.94. US 5224164 A, 29.06.93. US 5231666 A, 27.07.93. US 5337043 A, 09.08.94. US 5421006 A, 30.05.95. GB 2261538 A, 19.05.93. RU 2015575 C1, 30.06.94.

(85) Дата перевода заявки PCT на национальную фазу: 07.04.1997

(86) Заявка PCT:
US 95/11136 (01.09.1995)

(87) Публикация PCT:
WO 96/08092 (14.03.1996)

(98) Адрес для переписки:
129010, Москва, ул.Большая Спасская, 25 стр.3, ООО "Городисский и Партнеры", Емельянову Е.И.

(71) Заявитель:
Интел Корпорейшн (US)

(72) Изобретатель: Дерек Л.Дэвис (US)

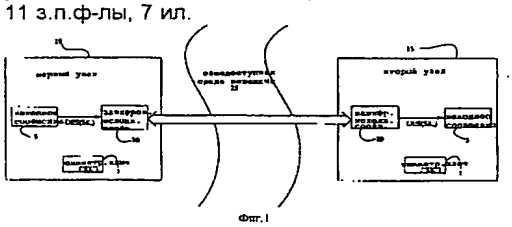
(73) Патентообладатель:
Интел Корпорейшн (US)

RU 2147790 C1

(54) ПЕРЕДАЧА ЛИЦЕНЗИИ НА ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ ЭЛЕМЕНТА АППАРАТНОГО ОБЕСПЕЧЕНИЯ

(57) Реферат:

Изобретение относится к лицензированию программных средств. Элемент аппаратных средств выполнен на интегральной схеме. Он предназначен для обеспечения соблюдения лицензионных ограничений. Такое соблюдение обеспечивается путем дистанционной передачи привилегий доступа для выполнения лицензированной программы от данного элемента аппаратных средств на интегральной схеме к другому аналогичному элементу. Элемент аппаратных средств на интегральной схеме содержит энергозависимую память, предназначенную для хранения уникальной выделенной пары ключей шифрования, цифровой сертификат устройства, предназначенный для аутентификации, и открытый ключ шифрования изготовителя вместе с криптографическим алгоритмом, блок обработки. Последний предназначен для выполнения криптографических алгоритмов при обработке информации, введенной в элемент аппаратных средств, и для передачи обработанной информации в энергозависимую память. Элемент содержит также генератор случайных чисел, предназначенный для генерирования уникальной выделенной пары ключей. 5 с. и 11 з.п.ф-лы, 7 ил.



Фиг.1

RU 2147790 C1

Изобретение относится к лицензированию программных средств. В частности, оно относится к устройству и способу для переноса привилегии доступа для выполнения программы лицензированных программных средств от санкционированного узла, имеющего первый элемент аппаратных средств, к несанкционированному узлу, имеющему второй элемент аппаратных средств, без нарушения лицензии конкретного пользователя.

Предшествующий уровень техники

На ранних этапах развития компьютерной техники при осуществлении коммерческих сделок в типовом случае использовалась централизованная универсальная вычислительная машина, имеющая ряд непрограммируемых ("немых") терминалов, подключенных к универсальной машине. С появлением малогабаритных более быстродействующих и более эффективных компьютеров большинство таких современных коммерческих систем отказались от своих централизованных универсальных вычислительных машин и перешли на использование ряда автономных компьютеров или распределенной сети (например, локальной сети), включающей в себя множество персональных компьютеров, причем каждый пользователь осуществляет управление своим собственным персональным компьютером.

Учитывая эту тенденцию к децентрализации, многие разработчики программного обеспечения лицензируют свои программные средства в соответствии с конкретной схемой лицензирования, обычно определяемой как "лицензия конкретного пользователя". Лицензия конкретного пользователя в общем случае позволяет предварительно определенному числу индивидуальных пользователей работать с конкретной программой определенным образом в течение конкретного времени. Таким образом, лицензия связана с выбранным числом пользователей, но не с определенным узлом. Для целей настоящего изобретения термин "узел" определяется как аппаратное средство интеллектуального характера, например компьютер, принтер, факсимильный аппарат и т.п. средство, предпочтительно предусматривающее настоящее изобретение. Первостепенной проблемой, связанной с лицензиями на программные средства для конкретных пользователей, является то, что при этом имеет место косвенное стимулирование несанкционированного использования и/или копирования лицензированного программного обеспечения, что наносит урон потенциальным доходам от лицензирования для разработчиков программных средств.

Несколько лет назад разработчики программных средств придумали способ защиты своих программных средств от использования и копирования вне норм лицензирования конкретных пользователей, в то время как коммерческие обладатели лицензий пытались существенно ослабить любую косвенную ответственность за несанкционированное использование или копирование лицензированных программных средств своим персоналом. Таким образом, как разработчики программных средств, так и коммерческие обладатели лицензий были заинтересованы в том, чтобы одинаковым образом препятствовать распространению программных средств вне рамок лицензий для конкретного пользователя.

В настоящее время согласие с лицензией на программные средства для конкретного пользователя осуществляется путем использования некоторого физического узла аппаратных средств, своеобразного "приемоответчика" (dongle). Этот узел упакован вместе с программой лицензированных программных средств и поставляется совместно с ними. Он в типовом случае связан с параллельным портом узла, например персонального компьютера. В различные моменты времени при своем выполнении лицензированная программа будет передавать сообщение санкционирования ("запрос") активному устройству, входящему в состав упомянутого приемоответчика. Это активное устройство обрабатывает запрос с использованием секретной информации (далее называемой "маркером действенности лицензии"), хранящейся в приемоответчике, и формирует ответное сообщение. Программа сравнивает этот ответ с ожидаемым ответом и разрешает дальнейшее выполнение программы, только если эти оба ответа идентичны.

Таким образом, хотя пользователь может скопировать лицензированную программу и загрузить ее во множество персональных компьютеров, однако только первый персональный компьютер, с которым соединен приемоответчик, будет обеспечивать выполнение этой программы. Для осуществления выполнения лицензированной программы на другом персональном компьютере приемоответчик необходимо физически удалить из первого персонального компьютера и соединить его с другим персональным компьютером. В результате будет иметь место запрет выполнения программы на первом персональном компьютере. Ясно, что множество инсталляций лицензированной программы не будет иметь отрицательных финансовых последствий для разработчика программы, так как число приемоответчиков, переданных коммерческому обладателю лицензии, в общем случае ограничено количеством лиц, которое согласовано при заключении лицензионного соглашения с конкретными пользователями программных средств.

Хотя вышеописанные приемоответчики обеспечивают совместимость с лицензией для конкретного пользователя, их использование имеет ряд недостатков. Один из них связан с необходимостью физической доставки такого "приемоответчика" покупателю. Таким образом, в то время как для повышения удобства и сокращения затрат на поставки предлагаются системы электронной доставки программных средств (называемые "поставками информации"), вышеуказанный подход, предусматривающий использование "материального средства", по-прежнему требует использования традиционной технологии доставки и связанных с ними затрат. При использовании описанных выше приемоответчиков в целях защиты финансовых интересов разработчиков программного обеспечения покупатель должен нести обременительные

RU 2147790 C1

RU 2147790 C1

обязанности, связанные со следующим: 1) непосредственно получать такой "приемоответчик" в конкретном месте и затем подсоединять его к узлу, прежде чем можно будет использовать лицензированную программу; 2) заказывать лицензированную программу заранее, до ее намеченного использования, чтобы дистрибьютор программных продуктов имел время на пересылку упомянутого "приемоответчика". В любом случае использование "приемоответчика" снижает эффективность и доступность систем распространения программных продуктов.

Другой недостаток указанного подхода состоит в том, что установка и снятие приемоответчика представляют собой процедуру, требующую дополнительных затрат времени. В случае коммерческой деятельности, критичной к временным затратам, необходимость замены приемоответчиков может повлиять на эффективность коммерческой деятельности в целом. Еще одним недостатком является то, что постоянное удаление и присоединение приемоответчика увеличивают вероятность его повреждения и функциональных отказов, что потребует приостановления коммерческой деятельности в ожидании поставки нового приемоответчика, прежде чем программное обеспечение можно будет использовать вновь.

Кроме того, недостатком является то, что хотя лицензия направлена на индивидуальных пользователей, приемоответчик в общем случае присоединяется к узлу. Таким образом, если пользователь перемещается с одной машины на другую (например, переходит на персональный компьютер, находящийся у него дома), то тем самым для него возникают препятствия использованию лицензированного программного обеспечения, если только данный пользователь не является сам владельцем приемоответчика.

Краткое изложение сущности изобретения

С учетом вышеизложенного, существует необходимость в создании криптографического устройства с функциональными возможностями электронного приемоответчика в виде элемента аппаратных средств на интегральной схеме. Соответственно задачей изобретения является создание криптографического устройства в виде элемента аппаратных средств на интегральной схеме, включающего в себя элемент памяти для внутреннего хранения уникального цифрового сертификата для использования при дистанционной аутентификации компонента на интегральной схеме.

Еще одной задачей изобретения является создание элемента аппаратных средств на интегральной схеме, обеспечивающего внутреннее генерирование уникальной пары открытого ключа и индивидуального ключа шифрования и хранение, по меньшей мере, индивидуального ключа, тем самым препятствуя его использованию вне элемента аппаратных средств.

Также задачей изобретения является создание элемента аппаратных средств для внутреннего хранения открытого ключа конкретного сообщества для обеспечения секретного обмена данными с другим аналогичным элементом аппаратных средств, контролируемым или изготовленным данным сообществом.

А также задачей изобретения является создание элемента аппаратных средств для обеспечения передачи лицензии на программное обеспечение, не требуя для этого постоянных физических манипуляций с аппаратными средствами.

Элемент аппаратных средств согласно изобретению содержит блок обработки для выполнения операций по идентификации и элемент памяти, включающий в себя энергонезависимую память для хранения уникальной пары открытого ключа и индивидуального ключа шифрования, цифрового сертификата для аутентификации пары ключей и открытого ключа выбранного сообщества (предпочтительно изготовителя элемента аппаратных средств) для обеспечения обмена данными между данным элементом аппаратных средств и другими аналогичными элементами данного изготовителя. Энергонезависимая память может также использоваться для хранения криптографических алгоритмов. Элемент аппаратных средств также содержит энергозависимую память для хранения информации, обрабатываемой блоком обработки, интерфейс для приема и для передачи информации в зашифрованном или расшифрованном формате от или соответственно к другим аналогичным элементам посредством шины передачи данных, а также генератор случайных чисел для формирования уникальной пары открытого ключа и индивидуального ключа шифрования.

Краткое описание чертежей

Задачи, признаки и преимущества настоящего изобретения поясняются в последующем детальном описании со ссылками на иллюстрирующие чертежи, на которых представлено следующее:

фиг. 1 - блок-схема, иллюстрирующая двунаправленный процесс шифрования и дешифрования с использованием симметричного ключа шифрования,

фиг. 2 - блок-схема, иллюстрирующая двунаправленный процесс шифрования и дешифрования с использованием асимметричного ключа шифрования,

фиг. 3 - блок-схема, иллюстрирующая процедуру цифровой сертификации полномочным органом,

фиг. 4 - блок-схема компьютерной системы, воплощающей в себе вариант осуществления изобретения,

фиг. 5 - блок-схема варианта осуществления настоящего изобретения,

фиг. 6 - блок-схема последовательности операций способа введения упомянутой пары и цифрового сертификата в элемент аппаратных средств,

фиг. 7A - 7C - блок-схемы последовательностей операций первого элемента аппаратных средств, устанавливающего связь с вторым элементом аппаратных средств для переноса маркера действенности лицензии между вторым элементом аппаратных средств, имеющего лицензированные привилегии, и первым элементом аппаратных средств.

RU 2147790 C1

RU 2147790 C1

Детальное описание вариантов осуществления изобретения

Настоящее изобретение относится к устройству и способу для обеспечения передачи лицензии на программные средства между соответственно конфигурированными элементами аппаратных средств и исключения при этом необходимости в использовании поставляемых материальных аппаратных средств. В нижеследующем описании различные признаки детально поясняются для обеспечения правильного понимания сущности изобретения. Вместе с тем, для специалистов в данной области техники должно быть ясно, что настоящее изобретение может быть реализовано на практике в виде различных других вариантов осуществления, чем те, которые проиллюстрированы в описании, без изменения при этом сущности и объема изобретения. Кроме того, хорошо известные схемы, элементы и т.п. детально не поясняются, чтобы излишне не загружать описание изобретения.

В нижеследующем подробном описании изобретения часто используются ряд терминов, относящихся к криптографии, для описания некоторых характеристик или свойств, что определяется ниже. Термин "ключ" представляет собой параметр кодирования и/или декодирования для обычного криптографического алгоритма. Более конкретно, ключ представляет собой последовательное распределение ("строку") двоичных данных длиной n битов, где n - произвольное число. Термин "сообщение" в общем случае определяется как информация (например, шифрованные адрес и данные ключей), которые должны передаваться в последовательности циклов шины. Информация может включать в себя запрос и ответный отклик. Термин "цифровой сертификат" определяется как информация, относящаяся к сообществу, осуществляющему информационный обмен, в типовом случае его открытый ключ шифрования, зашифрованная с использованием индивидуального ключа публичного уполномоченного органа (например, банка, правительственной организации, торговой ассоциации и т.п.). Термин " цифровая сигнатура" сходен по смыслу с термином "цифровой сертификат", но используется для аутентификации собственно сообщения, а не отправителя.

В последние годы все более необходимой становится передача цифровой информации из одного места в другое. В результате многие сообщества в настоящее время используют криптографическую технологию, так что информация может передаваться таким образом, что она представляется понятной и однозначно определенной для законного получателя, но совершенно неразборчивой и невоспринимаемой для незаконных получателей. В типовом случае криптографическая технология функционирует в соответствии с одним из двух общепринятых методов, а именно: криптография на основе симметричного ключа шифрования или криптография на основе асимметричного (или открытого) ключа шифрования или комбинация указанных технологий криптографии.

На фиг. 1 представлен пример осуществления способа криптографии с использованием симметричного ключа шифрования. Этот способ требует использования идентичного, т.е. симметричного секретного ключа шифрования (обозначаемого SK) 1 для шифрования исходного сообщения 5, подлежащего передаче между первым узлом 10 и вторым узлом 15, для получения шифрованного исходного сообщения 20 и для дешифрования зашифрованного исходного сообщения 20 для восстановления исходного сообщения 5. Такое шифрование и дешифрование выполняются с использованием широко известных традиционных криптографических алгоритмов, например, "Алгоритма Шифрования Данных", обычно называемого DES. Исходное сообщение 5 подвергается следующей обработке: (1) шифруется в первом узле 10, (2) передается от первого узла 10 во второй узел 15 через открытую среду передачи, например телефонные каналы и т.п., и (3) дешифруется во втором узле 15. Однако данный способ затруднительно поддерживать для большого числа пользователей, так как он требует предварительного определения секретных ключей шифрования (SK).

На фиг. 2 представлен пример осуществления способа с использованием асимметричного ключа шифрования. В этом способе два отдельных ключа (называемые "открытым ключом" и "индивидуальным ключом") используются раздельно для шифрования и дешифрования. Для установления двустороннего обмена данными между первым узлом 10 и вторым узлом 15 "открытый " ключ 16 из пары ключей второго узла 15 (обозначенный PUK2) хранится и в общем случае используется первым узлом 10 для шифрования исходного сообщения 30 согласно асимметричному алгоритму RSA, широко известному в криптографии. При этом формируется зашифрованное исходное сообщение 35, подлежащее передаче к второму узлу 15. Кроме того, в первом узле 10 хранится пара ключей первого узла, т. е. открытый ключ 11 и индивидуальный ключ 12.

"Индивидуальный" ключ 17 из пары ключей второго узла 15 (обозначенный PUK2) известен и используется исключительно вторым узлом 15 для различных целей, включая дешифрование зашифрованного сообщения 35 из первого узла 10 в соответствии с алгоритмом RSA, как показано на фиг. 2. Однако этот способ не защищен от попыток незаконных групп (например, осуществляющих промышленный шпионаж) выдать себя за законные сообщества (например, наемных работников или сотрудников совместных предприятий и т.п.) путем передачи мошеннических сообщений другим законным сообществам с целью внесения нарушений в действующий информационный поток или получения конфиденциальной информации. Поэтому обычно используются дополнительные протоколы для аутентификации сообщения и проверки легитимности сообщества, направившего сообщение.

Аутентификация отправителя (например, проверка того, что отправитель, использовавший открытый ключ шифрования, является действительно истинным

RU 2147790 C1

RU 2147790 C1

владельцем этого открытого ключа) представляет собой проблему при первоначальной установке информационных обменов между ранее неизвестными сторонами. Этой проблемы можно в общем случае избежать путем введения цифрового сертификата 45 в передаваемое сообщение 50. Цифровой сертификат 45 выпускается органом 55, наделенным взаимными полномочиями (например, банком, государственной организацией, торговой ассоциацией и т.п.) путем шифрования открытого ключа 11 узла, инициировавшего информационный обмен (PUK1), сигнатурным элементом (обозначенным SM) 58 с индивидуальным ключом (PRKTA) 57 этого полномочного органа 55, так что мошеннические попытки использовать PUK2 16 будут приводить в результате к нечитаемому отклику на переданное сообщение, сформированному его получателем. Выбор полномочного органа 55 зависит от сторон, участвующих в информационном обмене. Например, два лица, занятые в одной и той же коммерческой деятельности, могли бы оба доверять сертификатам, выпущенным некоторой корпоративной организацией, являющейся гарантом этой коммерческой деятельности. Наемным работникам двух независимых коммерческих организаций, однако, потребовались бы не только сертификаты соответствующих организаций-поручителей, но и сертификаты, например, от некоторой торгово-промышленной организации, которая регистрирует такие коммерческие сообщества.

При таком подходе для формирования передаваемого сообщения 50 одновременно выполняются множество операций. Так, исходное сообщение 40 шифруется с использованием симметричного секретного ключа (SK) 60 с помощью алгоритма DES, в результате чего формируется зашифрованное сообщение 65, которое вводится в передаваемое сообщение 50 вместе с цифровым сертификатом 45. Исходное сообщение 40 также обрабатывается с использованием алгоритма хэширования (перестановки) 70 (например, MD5) для формирования дайджеста (краткого изложения) 75 передаваемого сообщения. Дайджест 75 передаваемого сообщения дополнительно шифруется с использованием индивидуального ключа шифрования первого узла (PRK1) 12 для формирования цифровой сигнатуры 80, которая вводится в передаваемое сообщение 50. Дополнительно, симметричный ключ (SK) 60 шифруется с помощью открытого ключа шифрования второго узла (PUK2) 16 согласно алгоритму RSA, в результате чего формируется зашифрованный симметричный ключ "SKenc" 85, также вводимый в передаваемое сообщение 50.

Согласно фиг. 3 после приема сообщения 50, переданного первым узлом 10 через общедоступную среду передачи 25, второй узел 15 дешифрует зашифрованный симметричный ключ "SK_{enc}" 85 с помощью своего индивидуального ключа шифрования (PRK2) 17 и цифровой сертификат 45 с помощью открытого ключа (PUBTA) уполномоченного органа 55 для получения ключа SK 60 и ключа PUK1 11. Эти ключи SK и PUK1 60 и 11 используются для дешифрования зашифрованного исходного сообщения 65 и цифровой сигнатуры 80 для выделения дайджеста 75 переданного сообщения и исходного сообщения 40 соответственно. Исходное сообщение 40 затем обрабатывается с использованием алгоритма хэширования 85, идентичного выполнявшемуся в первом узле 10. Полученные результаты (определяемые как "дайджест принятого сообщения") 90 сравниваются с дайджестом 75 переданного сообщения 75. Если дайджест 75 переданного сообщения идентичен дайджесту 90 принятого сообщения, то информационный обмен между этими двумя правомочными узлами поддерживается.

На фиг. 4 представлен вариант осуществления компьютерной системы 100, использующей настоящее изобретение. Компьютерная система 100 содержит множество взаимодействующих с шиной компонентов, включая главный процессор 105, память 110, контроллер 115 ввода/вывода и криптографическое устройство, определенное здесь как "элемент аппаратных средств" 120. Множество компонентов системы, взаимодействующих с шиной, связаны между собой посредством системной шины, которая обеспечивает информационный обмен между указанными компонентами.

Следует иметь в виду, что, как хорошо известно в данной области техники, в компьютерной системе 100 может быть использовано более одного главного процессора, хотя на чертеже показан только один главный процессор 105. Кроме того, память 110 может содержать динамическое ЗУПВ, ПЗУ, ЗУПВ для сопряжения микропроцессора с телевизионным монитором и т.п. Память 110 хранит информацию, необходимую для использования главным процессором 105.

Контроллер ввода/вывода 115 представляет собой интерфейс между шиной ввода/вывода 135 и системной шиной 130, который обеспечивает канал связи (т. е. шлюз) для переноса информации между компонентами, связанными с системной шиной 130 или с шиной ввода/вывода 135. Шина ввода/вывода 135 переносит информацию по меньшей мере в одно периферийное устройство (или от него) в компьютерной системе 100, включая, без каких-либо ограничений, дисплей 140 (например, ЭЛТ, жидкокристаллический дисплей и т.п.) для отображения изображений, буквенно-цифровое устройство ввода 145 (например, буквенно-цифровая клавиатура и т.п.) для ввода информации и выбора команд для главного процессора 105, устройство управления 150 курсором (например, манипулятор типа "мышь", шар трассировки, вспомогательная сенсорная клавиатура и т.п.) для управления перемещением курсора, устройство массовой памяти 155 (например, магнитные ленты, дисководы на жестких дисках, на гибких дисках и т.п.) для хранения информации, устройство передачи и приема информации 160 (например, факсимильный аппарат, принтер, сканер и т.п.) для передачи информации от компьютерной системы 100 к другому устройству и для приема

RU 2147790 C1

RU 2147790 C1

информации от другого устройства и устройство 165 для изготовления печатных копий (например, плоттер, принтер и т.п.) для получения материального визуального представления информации. Ясно, что компьютерная система, показанная на фиг. 4, может использовать некоторые или все из перечисленных компонентов или иные компоненты, помимо показанных на чертеже.

Как показано на фиг.5, в одном из вариантов осуществления изобретения элемент аппаратных средств 120 связан с системной шиной 130, устанавливающей канал связи с главным процессором 105, а также с памятью и контроллерами ввода/вывода (не показаны). Элемент аппаратных средств 120 содержит одиночную интегральную схему в форме кристалла 121 (например, микроконтроллер), заключенного в корпус 122 интегральной схемы, предпочтительно герметичный, для защиты кристалла 121 от повреждения и загрязнений. Кристалл 121 содержит блок обработки 123, соединенный с элементом памяти 124, интерфейсом шины 125 и генератором чисел 126. Интерфейс шины 125 обеспечивает информационный обмен между элементом аппаратных средств 120 с любым другим устройством (например, главным процессором, другим подобным элементом аппаратных средств в другом устройстве и т.п.). Блок обработки 123 выполняет вычисления внутренним образом в защищенной среде внутри кристалла 121, обеспечивая подтверждение правильности соединения с санкционированным получателем информации. Такие вычисления включают в себя выполнение определенных алгоритмов и протоколов, запуск электронных схем (например, генератора чисел 126, предпочтительно генератора случайных чисел) для генерирования специфической для устройства пары открытого ключа и индивидуального ключа шифрования и т.п. Блок обработки 123 находится внутри кристалла 121 для предотвращения возможности доступа к индивидуальному ключу путем использования воздействия вирусов, что представляет собой обычный метод нарушения работы компьютерной системы для получения ее индивидуального ключа шифрования и другой информации.

Элемент памяти 124 включает в себя энергонезависимую память 127 для запоминания соответствующих криптографических алгоритмов, таких как RSA, DES, пары открытого и индивидуального ключей шифрования 127a, цифрового сертификата для проверки аутентичности пары ключей (обозначаемого DC) 127b и открытого ключа шифрования изготовителя компонента на интегральных схемах (PUKM) 127c для обеспечения обмена данными между компонентом на интегральных схемах и другим аналогичным устройством, изготовленным тем же изготовителем (более детально это рассмотрено со ссылками на фиг. 6). Эта энергонезависимая память 127 используется главным образом потому, что она обеспечивает сохранение своего содержимого и в тех случаях, когда отсоединяется источник питания. Блок памяти 124 также включает в себя ЗУПВ 128 для хранения результатов, полученных в результате обработки в блоке обработки 123.

Хотя элемент аппаратных средств 120 реализован как периферийное устройство на системной шине 130 для обеспечения большей секретности, однако следует иметь в виду, что элемент аппаратных средств 120 может быть реализован и иными путями на уровне структуры персонального компьютера, например как контроллер диска или плата стандарта PCMCIA (Стандарт ассоциации по интерфейсу плат памяти для персональных компьютеров), для автоматического дешифрования и/или шифрования информации, вводимой и выводимой с жесткого диска. Другим возможным вариантом осуществления является выполнение элемента аппаратных средств как компонента мульти-кристального модуля, включающего в себя главный процессор, как описано ниже. Кроме того, хотя элемент аппаратных средств описан в связи со структурой персонального компьютера, ясно, что такой элемент аппаратных средств может быть реализован в узле таком, как факсимильный аппарат, принтер и т.п., или в канале связи между компьютером и периферийным устройством ввода/вывода.

На фиг. 6 представлена блок-схема последовательности операций при реализации настоящего изобретения. Сначала, на этапе 100, изготавливается кристалл элемента аппаратных средств в соответствии с любым соответствующим способом изготовления полупроводниковых компонентов, хорошо известным из уровня техники. Затем кристалл герметизируется в полупроводниковом корпусе с образованием собственно элемента аппаратных средств (этап 105). Элемент аппаратных средств устанавливается в систему сертификации, которая устанавливает электрическую и механическую связь между элементом аппаратных средств и системой сертификации (этап 110). Система сертификации содержит линию связи, связанную с платой печатной схемы, для генерирования и приема электрических сигналов, используемых для сертификации элемента аппаратных средств. Система сертификации также содержит устройство хранения данных (например, базу данных) ранее сформированных открытых ключей шифрования, необходимого для обеспечения генерирования уникального ключа. Затем система сертификации подает питание на элемент аппаратных средств, который запитывает генератор случайных сигналов, генерирующий уникальную для устройства пару открытого и индивидуального ключей шифрования внутренним образом внутри элемента аппаратных средств (этап 115).

После того как пара открытого и индивидуального ключей шифрования сформирована внутри элемента аппаратных средств, эта пара ключей шифрования передается в систему сертификации (этап 120). Открытый ключ сравнивается с ранее сформированными открытыми ключами для ранее изготовленных элементов аппаратных средств, хранящимися в устройстве хранения данных (этап 125). В маловероятном случае, если этот открытый ключ идентичен одному из ранее сформированных открытых ключей шифрования (этап 130), то элемент аппаратных средств получает соответствующий сигнал от системы

RU 2147790 C1

RU 2147790 C1

сертификации для генерирования другой такой пары ключей шифрования (этап 135), и этот процесс продолжается, начиная с этапа 120, для обеспечения уникального характера пары генерируемых открытого и индивидуального ключей шифрования.

В случае, если открытый ключ шифрования уникален, то устройство хранения данных обновляется записью этого уникального открытого ключа (этап 140). После этого на этапе 145 система сертификации создает уникальный сертификат устройства, подтверждающий аутентичность пары ключей (далее называемый "сертификатом устройства, предназначенным для аутентификации"). Сертификат устройства, предназначенный для аутентификации, будет включать, по меньшей мере, открытый ключ шифрования устройства, зашифрованный в цифровом виде секретным индивидуальным ключом изготовителя (т.е. иными словами, осуществляется шифрование открытого ключа устройства индивидуальным ключом шифрования изготовителя). Этот сертификат устройства, предназначенный для аутентификации, вместе с в принципе известным открытым ключом изготовителя вводятся в элемент аппаратных средств (этап 150), и элемент аппаратных средств программирует уникальную пару открытого и индивидуального ключей шифрования, сертификат устройства, предназначенный для аутентификации, и открытый ключ изготовителя в своей энергонезависимой памяти (этап 155). Ясно, что может быть использован открытый ключ шифрования другого сообщества (например, дистрибьютора) вместо ключа изготовителя, что требует модифицирования и сертификата устройства, предназначенного для аутентификации. К данному моменту технологического процесса обеспечивается физическая уникальность элемента аппаратных средств, который теперь может обеспечивать секретное установление обмена информационными данными с другим таким элементом аппаратных средств.

После того как элемент аппаратных средств изготовлен, он вводится в электронное устройство, такое как компьютерная система, показанная на фиг. 4. Это осуществляется путем установления секретного канала передачи информации между лицом, предоставляющим лицензию, и элементом аппаратных средств на основе процедур аутентификации, включающих запрос и ответ, а также другие хорошо известные процедуры. После того как обеспечен секретный канал обмена информацией, в память элемента аппаратных средств по этому каналу загружается маркер действенности лицензии. Ясно, что маркер лицензии может быть введен в множество элементов аппаратных средств и будет существовать в "истинном" или "неподтвержденном" состоянии, причем маркер лицензии будет подтверждаться или не подтверждаться, вместо того, чтобы его физически переносить от одного элемента аппаратных средств к другому.

На фиг. 7А и 7В представлен вариант осуществления взаимной дистанционной идентификации аутентичности двух элементов аппаратных средств. На этапе 200 устанавливается связь между "несанкционированным" первым узлом (т.е. узлом, которому в данный момент времени не разрешено использовать лицензированное программное обеспечение), содержащим первый элемент аппаратных средств, и вторым санкционированным узлом, содержащим второй элемент аппаратных средств, которому разрешено использовать лицензированное программное обеспечение. Этот канал связи может устанавливаться посредством любых обычных средств, например модемов, сетей и т.п. Первый элемент аппаратных средств выдает сообщение, включающее в себя его уникальный сертификат устройства, предназначенный для аутентификации, второму элементу аппаратных средств (этап 205). Поскольку открытый ключ шифрования изготовителя (PUKM) запрограммирован в энергонезависимой памяти обоих элементов аппаратных средств, то второй элемент аппаратных средств дешифрует сертификат устройства, предназначенный для аутентификации, с помощью открытого ключа шифрования изготовителя (PUKM) для получения открытого ключа шифрования первого элемента аппаратных средств (этап 210). После этого на этапах 215-220 осуществляются операции, аналогичные тем, которые были описаны для этапов 205-210, так что первый элемент аппаратных средств получает открытый ключ шифрования (PUK2) второго элемента аппаратных средств.

Затем на этапах 225-230 с использованием полученного открытого ключа шифрования первого элемента аппаратных средств второй элемент аппаратных средств шифрует сообщение запроса согласно выбранному криптографическому алгоритму (например, RSA) и передает сообщение запроса первому элементу аппаратных средств. На этапе 235 и 240 первый элемент аппаратных средств дешифрует сообщение запроса с использованием своего индивидуального ключа (PRK1) и генерирует ответное сообщение путем шифрования дешифрованного сообщения запроса с использованием открытого ключа шифрования второго элемента аппаратных средств (PUK2) и передает ответное сообщение второму элементу аппаратных средств. Затем второй элемент аппаратных средств дешифрует полученный ответ с использованием своего индивидуального ключа шифрования (PUK1), как это было ранее определено путем дешифрования ранее переданного сертификата устройства изготовителя (этап 245). На этапе 250 второй элемент аппаратных средств сравнивает исходное сообщение запроса с дешифрованным ответным сообщением, и если они не идентичны, то осуществление связи прекращается (этап 255). В противном случае на этапах 260-290 осуществляется процедура формирования и обработки запроса/ответа, подобная осуществлявшейся на этапах 225-260, для проверки того, что второй элемент аппаратных средств действительно принял информацию, переданную от первого элемента аппаратных средств. Успешное завершение этих этапов (225-290) гарантирует, что оба элемента аппаратных средств аутентичны и

RU 2147790 C1

RU 2147790 C1

информационный обмен между ними защищен (этап 295).

На фиг. 7С представлен вариант осуществления процедуры защищенного переноса маркера действенности лицензии от второго элемента аппаратных средств первому элементу аппаратных средств при осуществлении защищенной процедуры информационного обмена. После установления защищенной (секретной) связи первый элемент аппаратных средств запрашивает второй элемент аппаратных средств, обладает ли тот маркером действенности лицензии (этап 300). Если система, содержащая второй элемент аппаратных средств, не имеет маркера действенности лицензии (этап 305), то процедура связи между этими элементами аппаратных средств прекращается (этап 310). Однако если система, содержащая второй элемент аппаратных средств, имеет маркер действенности лицензии, то она передает соответственно сообщение первому элементу аппаратных средств (этап 315).

После приема этого сообщения первый элемент аппаратных средств инициирует запрос переноса маркера действенности лицензии, позволяющий первому элементу аппаратных средств использовать лицензированное программное обеспечение (этап 320). Второй элемент аппаратных средств отвечает на запрос переноса путем переноса маркера действенности лицензии, обуславливающего потерю им своих лицензированных привилегий (этап 325). Первый элемент аппаратных средств получает указанный маркер действенности лицензии и запоминает этот маркер в своей энергонезависимой памяти, и затем он должен передать сообщение второму элементу аппаратных средств о том, что он принял маркер действенности лицензии, позволяющий ему использовать свою копию упомянутого программного обеспечения (этап 330). В этот момент информационный обмен будет закончен (этап 335).

Ясно, что может быть получен дополнительный уровень целостности протокола за счет введения последовательности запрос/ответ между этапами 320 и 325 и между этапами 325 и 330. Это позволяет исключить "повтор" предыдущих событий переноса маркера лицензии.

Одновременно с осуществлением связи между первым и вторым элементами аппаратных средств каждый такой элемент аппаратных средств будет запоминать содержимое своих передач в энергонезависимой памяти в качестве контрольной регистрации. Таким образом, в случае разъединения связи, после того как второй элемент аппаратных средств блокировал свою копию, но перед тем как первый элемент аппаратных средств задействовал свою копию, оба эти элемента аппаратных средств могут просмотреть свои контрольные регистрации после восстановления связи для определения того, какой элемент аппаратных средств (если таковой имеется) имеет разрешение использовать лицензированное программное обеспечение.

Настоящее изобретение, описанное выше, может быть осуществлено на практике различными путями с использованием самых различных конфигураций. Хотя настоящее изобретение было описано на примере некоторых вариантов его осуществления, специалисты в данной области техники могут предложить другие подобные варианты, не выходя за пределы сущности и объема изобретения. Изобретение должно поэтому оцениваться в терминах пунктов формулы изобретения.

Формула изобретения:

1. Элемент аппаратных средств, выполненный на интегральной схеме в корпусе и предназначенный для шифрования и дешифрования информации, содержащий блок обработки, предназначенный для внутренней обработки информации, энергонезависимую память, предназначенную для хранения данных, для хранения уникальной пары ключей шифрования, цифрового сертификата, предназначенного для аутентификации, и открытого ключа шифрования изготовителя элемента, причем энергонезависимая память связана с блоком обработки, память с произвольной выборкой, предназначенную для хранения информации, обработанной блоком обработки, причем память с произвольной выборкой данных связана с блоком обработки, генератор чисел для генерирования уникальной пары ключей шифрования, связанный с блоком обработки, и шинный интерфейс, предназначенный для обеспечения информационного обмена с элементом, при этом шинный интерфейс связан с блоком обработки.

2. Элемент по п.1, отличающийся тем, что упомянутый цифровой сертификат, предназначенный для аутентификации, представляет собой открытый ключ шифрования изготовителя элемента, зашифрованный индивидуальным ключом шифрования этого изготовителя.

3. Элемент по п.1, отличающийся тем, что энергонезависимая память, кроме того, содержит криптографический алгоритм.

4. Элемент по п.1, отличающийся тем, что генератор чисел выполнен в виде генератора случайных чисел.

5. Элемент по п.1, отличающийся тем, что шинный интерфейс связан с шиной для обеспечения канала связи с упомянутым элементом на интегральной схеме и для обеспечения возможности элементу на интегральной схеме дешифровать и запоминать информацию, переданную к нему, и шифровать и передавать информацию от него.

6. Элемент аппаратных средств, выполненный на интегральной схеме и предназначенный для шифрования и дешифрования информации, содержащий блок обработки, предназначенный для внутренней обработки указанной информации, энергонезависимую память, предназначенную для хранения уникальной пары ключей шифрования, сертификата устройства изготовителя элемента на интегральной схеме и открытого ключа шифрования упомянутого изготовителя, причем энергонезависимая память связана с блоком обработки, память с произвольной выборкой, предназначенную для хранения указанной информации и связанную с блоком обработки, генератор случайных чисел, предназначенный для генерирования

RU 2147790 C1

RU 2147790 C1

информации для формирования уникальной пары ключей шифрования, причем упомянутый генератор случайных чисел связан с блоком обработки, и шинный интерфейс, предназначенный для обеспечения информационного обмена с элементом на интегральной схеме, при этом упомянутый шинный интерфейс связан с блоком обработки.

7. Элемент по п.6, отличающийся тем, что упомянутый шинный интерфейс обеспечивает канал связи для обеспечения возможности элементу на интегральной схеме осуществлять дешифрование и запоминание информации, передаваемой к нему, а также шифрование и передачу информации, передаваемой от него.

8. Компьютерная система, предназначенная для шифрования и дешифрования информации, содержащая главный процессор и память для хранения программы, взаимодействующие с системной шиной, отличающаяся тем, что содержит элемент аппаратных средств, связанный с системной шиной и предназначенный для дешифрирования информации, поступающей в элемент аппаратных средств, и для шифрования информации, выдаваемой из элемента аппаратных средств, причем элемент аппаратных средств содержит блок обработки, предназначенный для обработки вводимой и выводимой информации внутри элемента аппаратных средств, элемент памяти, связанный с блоком обработки и предназначенный для хранения уникальной пары ключей шифрования, сертификата устройства изготовителя элемента аппаратных средств, открытого ключа шифрования изготовителя и вводимой и выводимой информации, генератор чисел, связанный с блоком обработки и предназначенный для генерирования упомянутой уникальной пары ключей шифрования, и шинный интерфейс, связанный с блоком обработки.

9. Система по п.8, отличающаяся тем, что элемент памяти включает в себя энергонезависимую память для сохранения упомянутой уникальной пары ключей шифрования в случае отсоединения питания от упомянутой энергонезависимой памяти.

10. Система по п.9, отличающаяся тем, что упомянутый элемент памяти предназначен для хранения криптографического алгоритма.

11. Компьютерная система, предназначенная для шифрования и дешифрирования информации, содержащая память, предназначенную для хранения, по меньшей мере, одной программы шифрования и дешифрирования, главный процессор, предназначенный для выполнения упомянутых программ шифрования и дешифрирования, системную шину, предназначенную для связи главного процессора и памяти, элемент аппаратных средств, связанный с системной шиной, предназначенный для внутреннего дешифрирования информации, вводимой от удаленного устройства, и шифрования информации, выдаваемой удаленному устройству, причем упомянутый элемент аппаратных средств включает в себя блок обработки упомянутой вводимой и выводимой информации в упомянутом элементе аппаратных средств, энергонезависимую память, предназначенную для хранения уникальной выделенной пары ключей шифрования, сертификата устройства для аутентификации и открытого ключа шифрования изготовителя, причем все эти данные предназначены для использования при дешифрировании упомянутой вводимой информации и шифрования упомянутой выводимой информации, при этом энергонезависимая память связана с упомянутым блоком обработки, энергозависимую память, предназначенную для временного хранения упомянутой вводимой и выводимой информации, обрабатываемой блоком обработки, генератор случайных чисел для генерирования упомянутой уникальной пары ключей шифрования, и шинный интерфейс, предназначенный для обеспечения связи между данной системой и удаленной системой, связанный с упомянутым блоком обработки.

12. Система по п.11, отличающаяся тем, что энергозависимая память предназначена для хранения, по меньшей мере, одного криптографического алгоритма.

13. Способ для аутентификации пары элементов аппаратных средств, заключающийся в том, что устанавливают канал связи между первым и вторым элементами аппаратных средств, осуществляют аутентификацию упомянутых первого и второго элементов аппаратных средств, передают сообщение запроса то первого элемента аппаратных средств второму элементу аппаратных средств для определения того, обладает ли второй элемент аппаратных средств маркером действенности лицензии, генерируют запрос переноса от первого элемента аппаратных средств к второму элементу аппаратных средств, при условии наличия маркера действенности лицензии у второго элемента аппаратных средств осуществляют перенос маркера действенности лицензии от второго элемента аппаратных средств к первому элементу аппаратных средств, генерируют сообщение приема маркера от первого элемента аппаратных средств к второму элементу аппаратных средств после приема маркера действенности лицензии.

14. Способ по п.13, отличающийся тем, что при аутентификации передают уникальный сертификат устройства, хранящегося в первом элементе аппаратных средств, к второму элементу аппаратных средств, дешифрируют уникальный сертификат устройства для получения открытого ключа шифрования первого элемента аппаратных средств, предназначенного для осуществления информационного обмена с первым элементом аппаратных средств и его аутентификации, передают уникальный сертификат устройства, запомненный во втором элементе аппаратных средств, к первому элементу аппаратных средств, дешифрируют уникальный сертификат устройства для получения открытого ключа шифрования второго элемента аппаратных средств, предназначенного для осуществления информационного обмена с вторым элементом аппаратных средств и его аутентификации, генерируют сообщение запроса, шифруемое открытым ключом шифрования первого элемента аппаратных

RU 2147790 C1

RU 2147790 C1

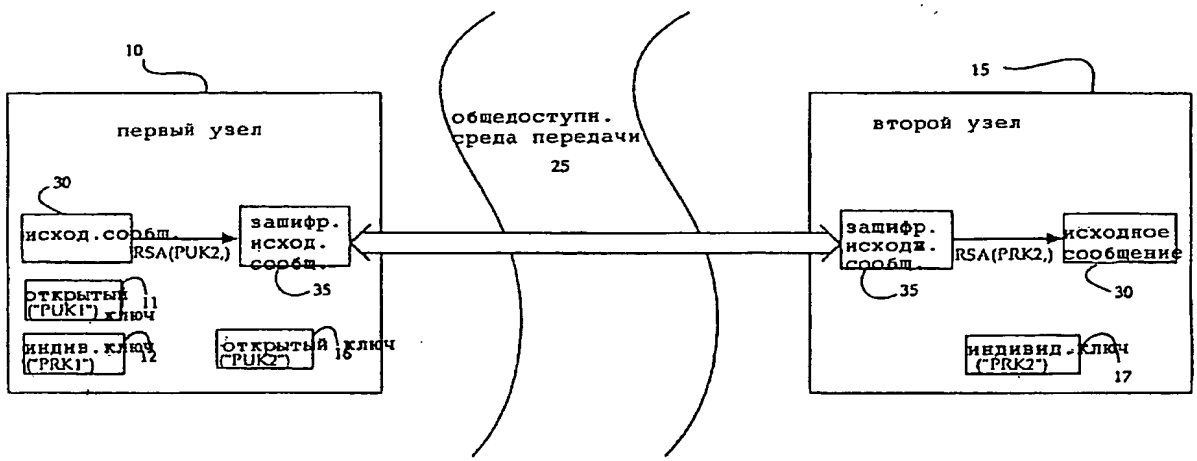
средств, передают сообщения запроса второму элементу аппаратных средств, дешифрируют сообщение запроса и формируют ответ на сообщение запроса вторым элементом аппаратных средств, генерируют сообщение запроса, шифруемое открытым ключом шифрования второго элемента аппаратных средств, передают сообщение запроса первому элементу аппаратных средств, дешифрируют сообщение запроса и формируют ответ на это сообщение запроса первым элементом аппаратных средств.

15. Способ по п.14, отличающийся тем, что получают открытый ключ шифрования первого элемента аппаратных средств, получают открытый ключ шифрования второго элемента аппаратных средств для определения того, что информационный обмен между первым и вторым элементами аппаратных средств является защищенным, осуществляют обмен сообщением запроса и сообщением ответа между первым элементом аппаратных средств и вторым элементом аппаратных средств.

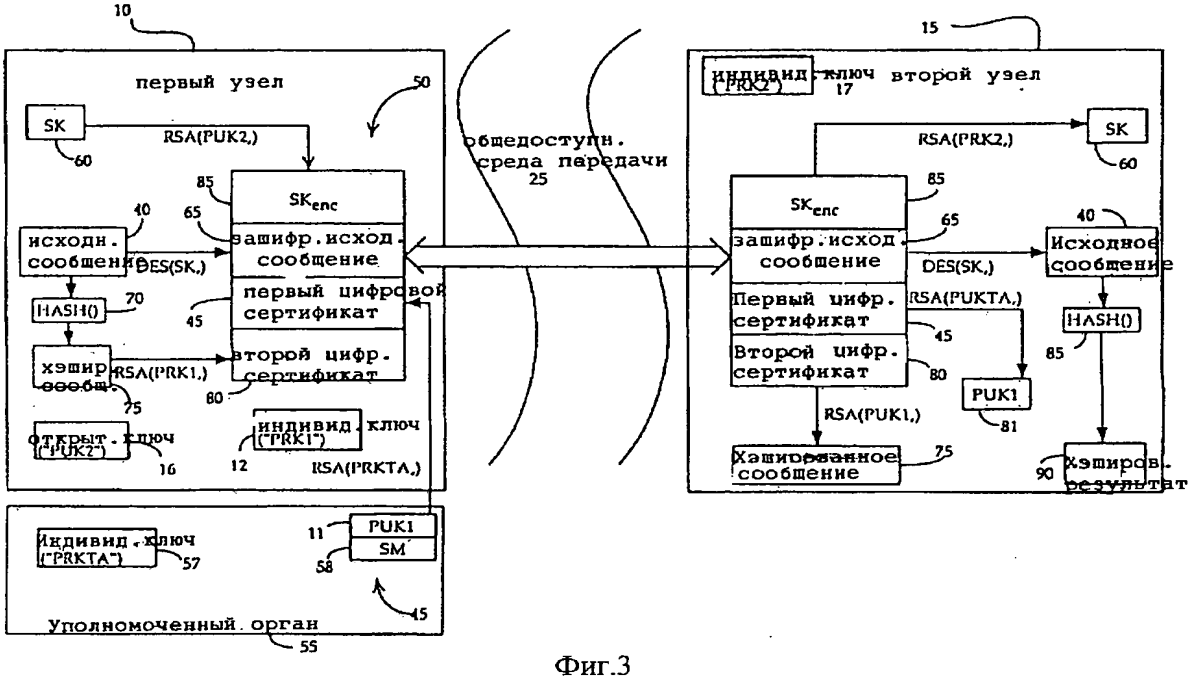
16. Способ по п.13, отличающийся тем, что перед генерированием запроса переноса дополнительно определяют вторым элементом аппаратных средств, обладает ли он маркером действенности лицензии, и при этом прекращают осуществление связи перед сообщением запроса при условии того, что второй элемент аппаратных средств не обладает маркером действенности лицензии, и генерируют сообщение ответа на сообщение запроса перед пересылкой маркера действенности лицензии при условии того, что второй элемент аппаратных средств обладает маркером действенности лицензии.

RU 2147790 C1

RU 2147790 C1



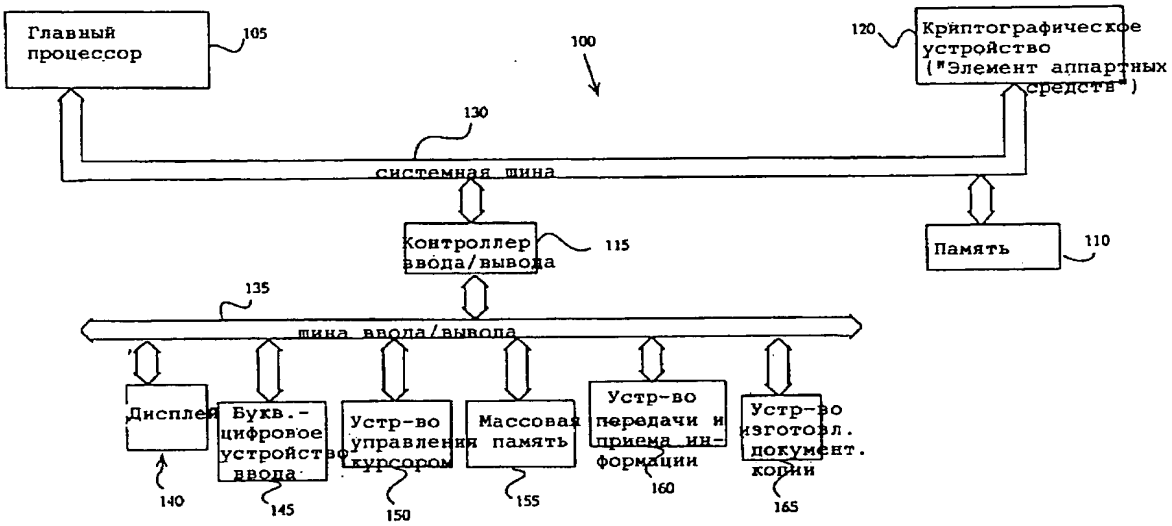
Фиг.2



Фиг.3

RU 2147790 C1

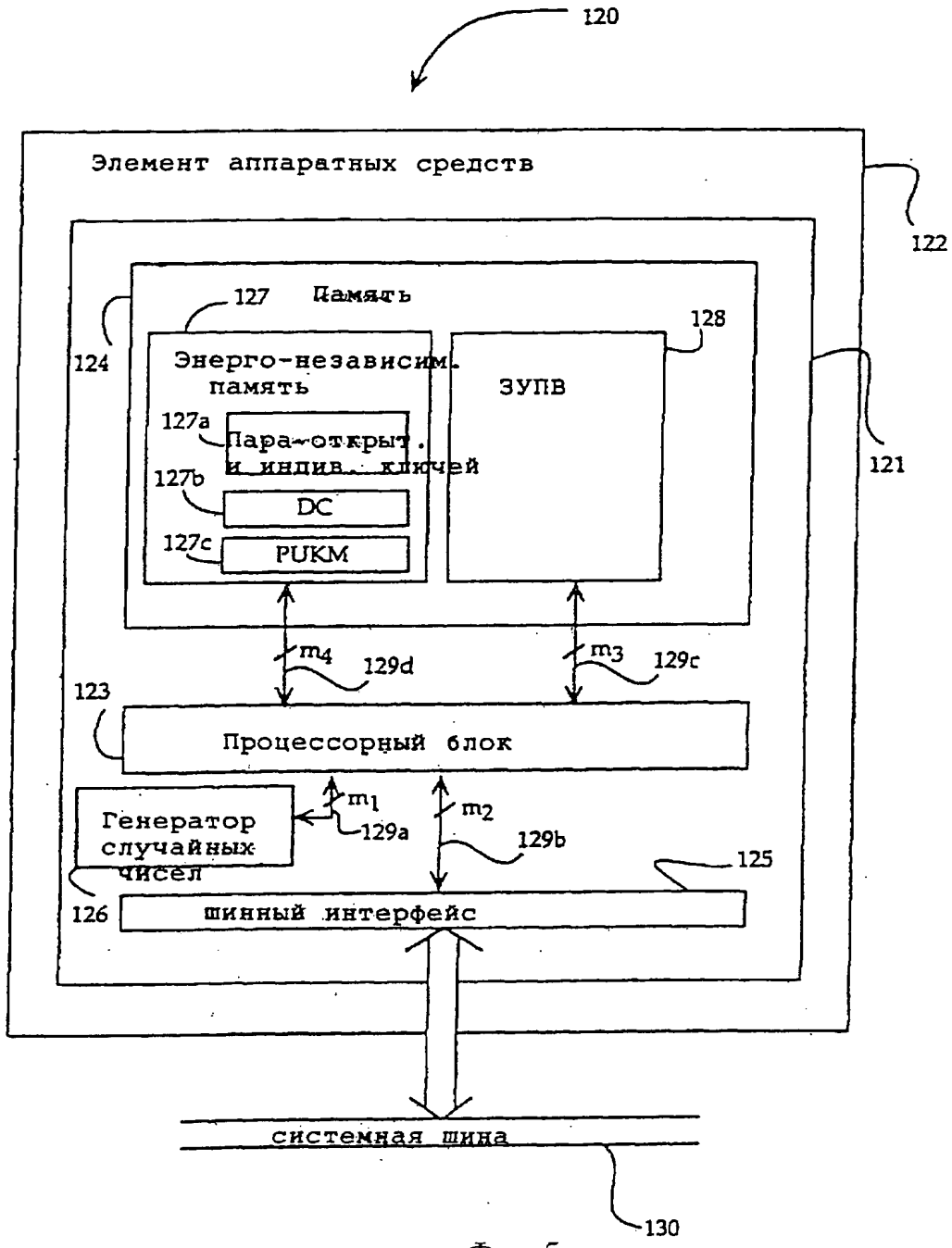
RU 2147790 C1



Фиг.4

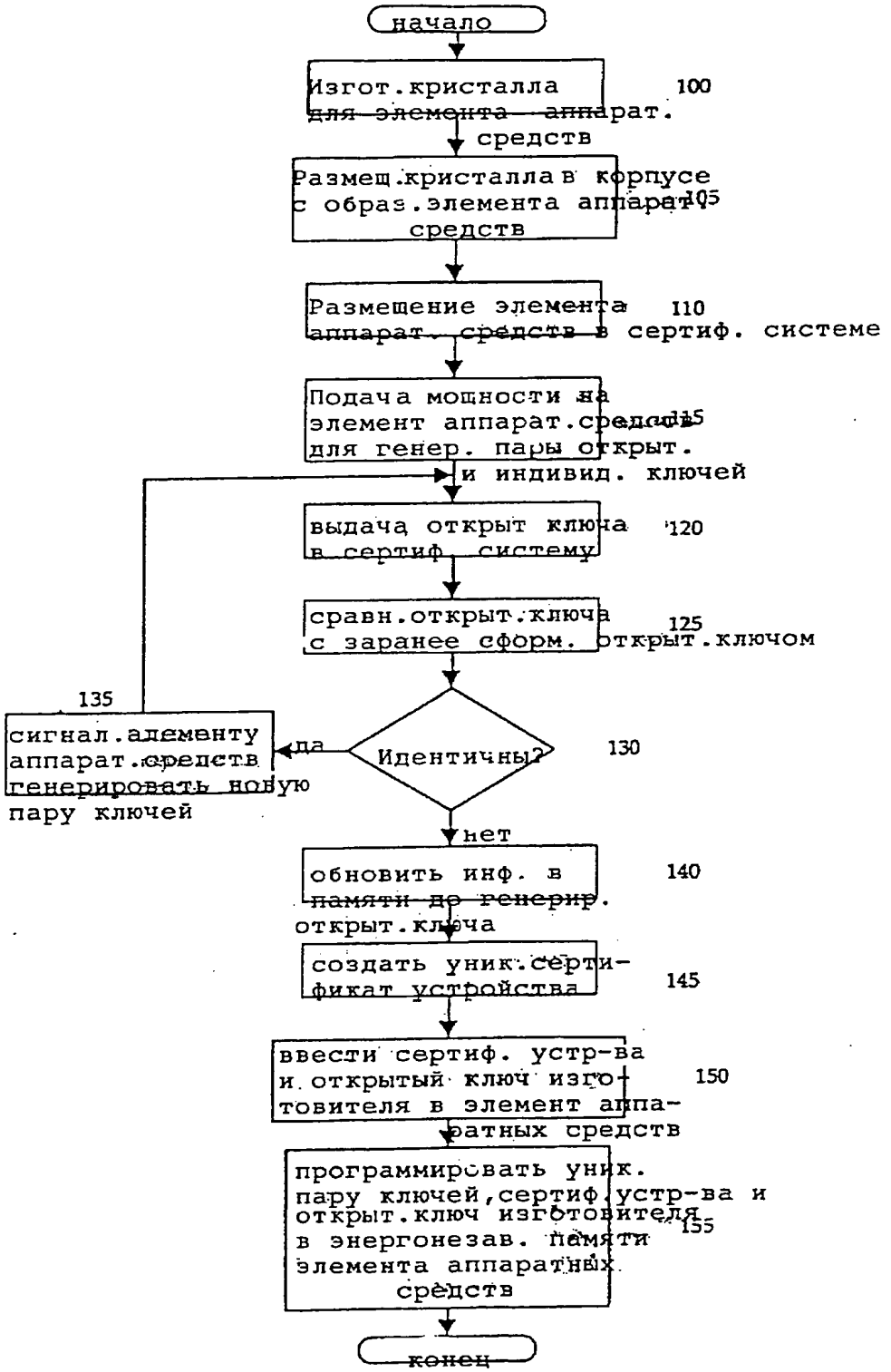
RU 2147790 C1

RU 2147790 C1



Фиг.5

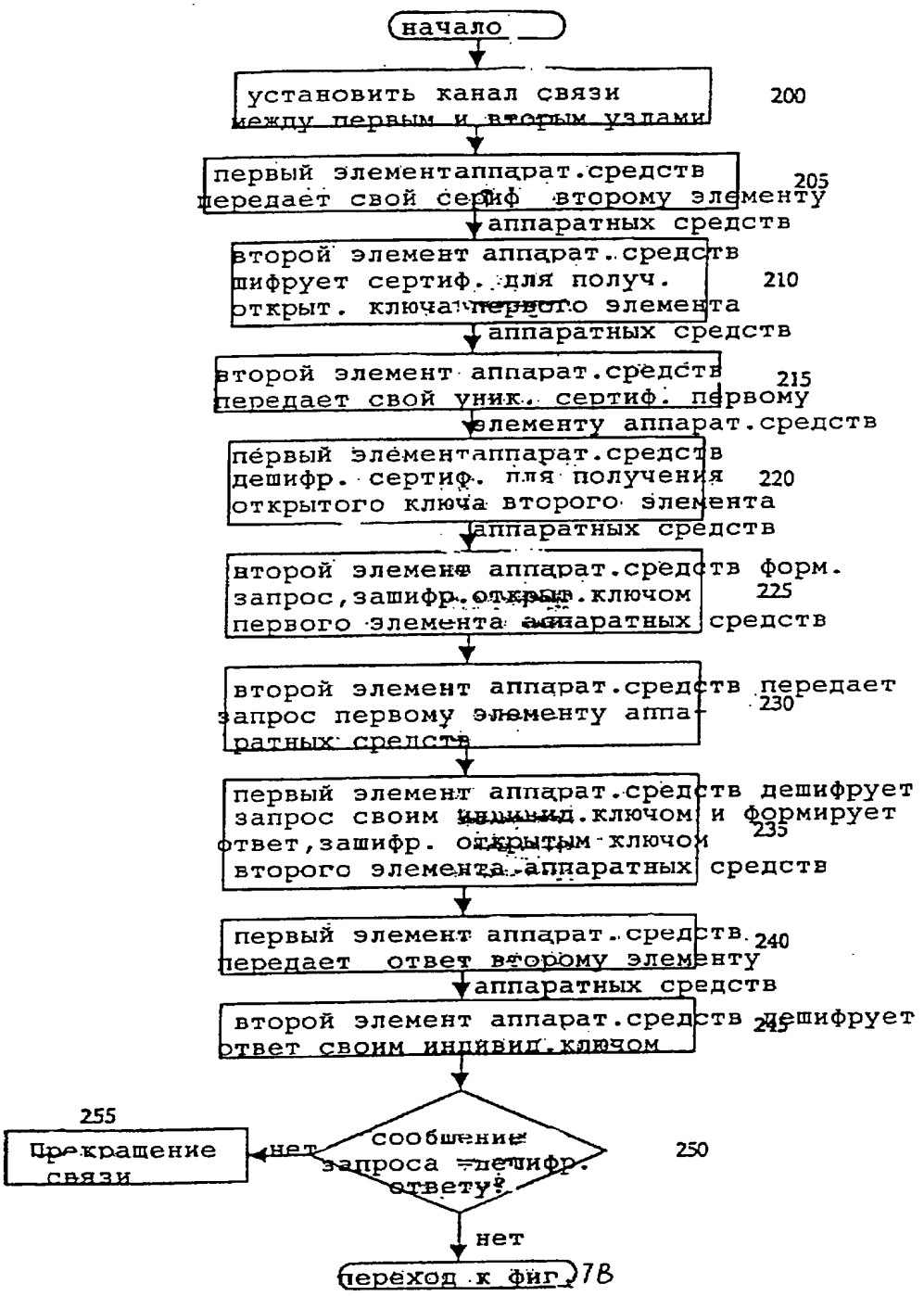
RU 2147790 C1



Фиг.6

RU 2147790 C1

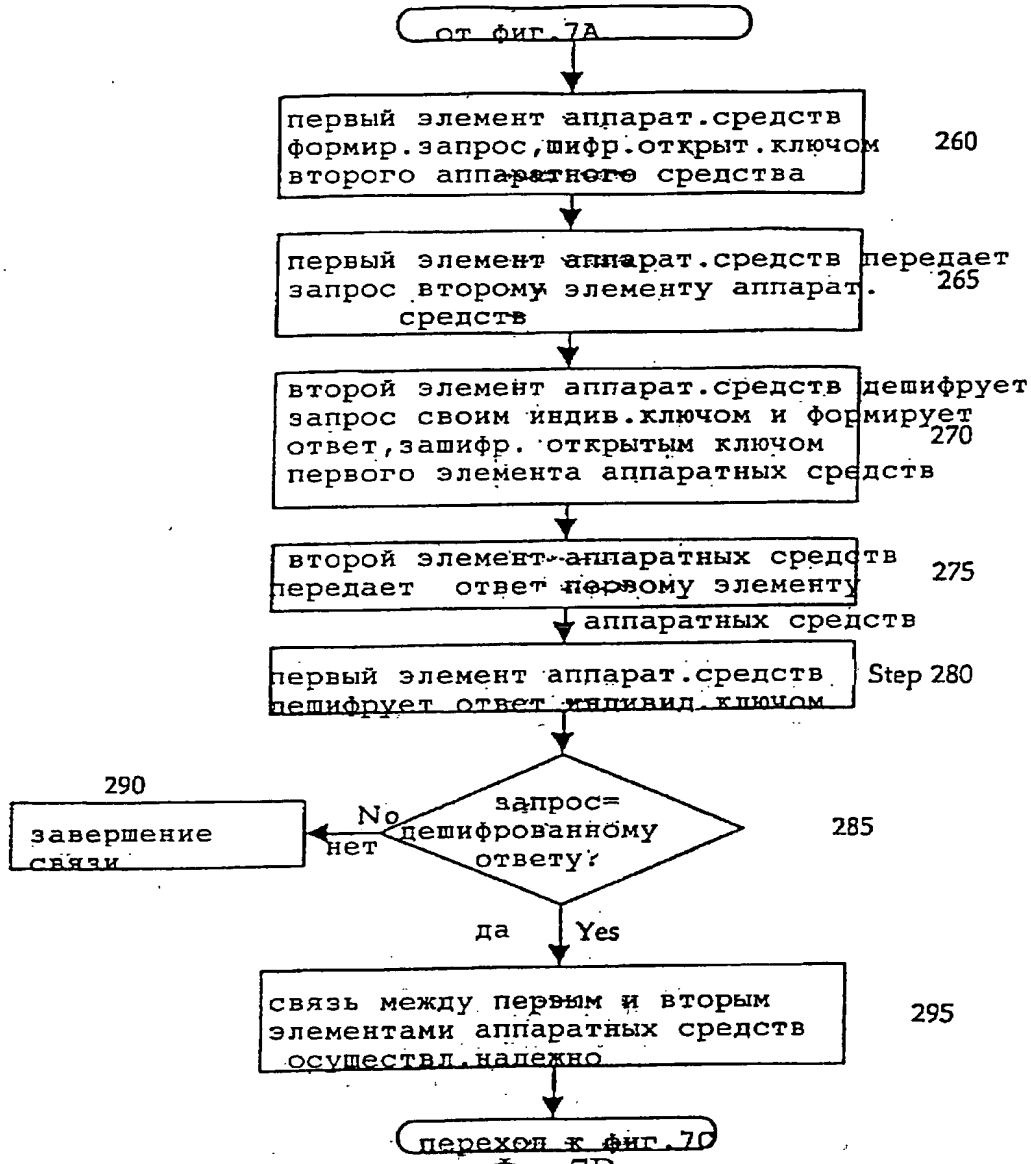
RU 2147790 C1



Фиг.7А

RU 2147790 C1

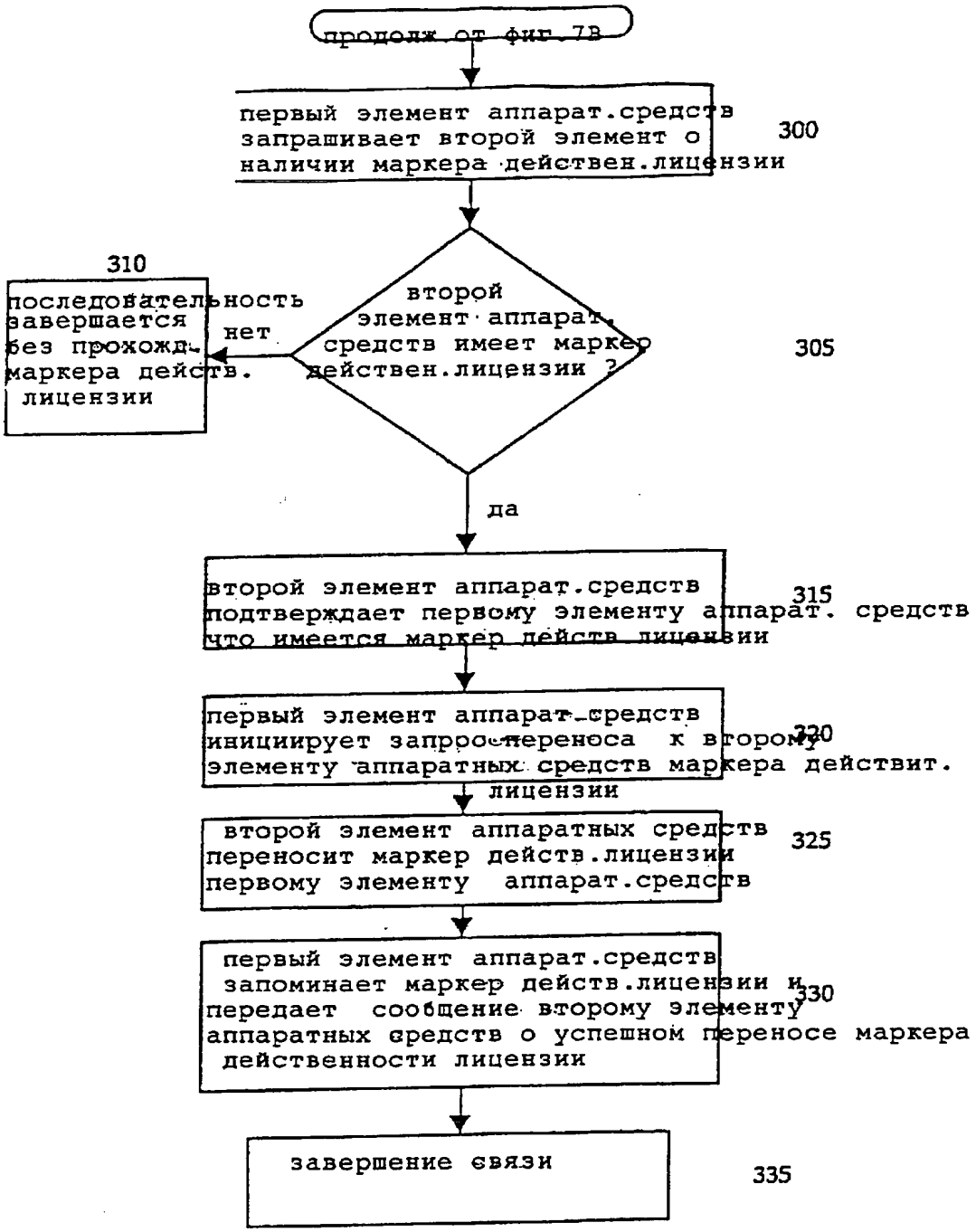
RU 2147790 C1



Фиг.7В

RU 2147790 C1

RU 2147790 C1



Фиг.7С

RU 2147790 C1

RU 2147790 C1